digital.ai™ continuous testing™

Digital.ai Continuous Testing

Livrer des applications de haute qualité en effectuant des tests rapidement et à l'échelle

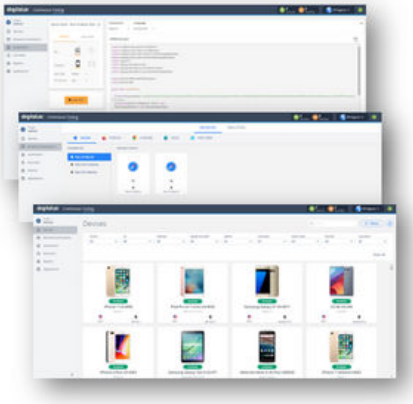
Les priorités organisationnelles évoluent. La demande d'applications et produits toujours plus performants et rapides augmente à mesure que les entreprises placent leur client au cœur de leur transformation numérique.

Les équipes chargées des tests et de l'assurance qualité doivent tester efficacement leurs applications web et mobiles afin de détecter les défauts dès le début du cycle de développement et les corriger rapidement. Egalement, ces équipes doivent s'assurer que la couverture de code globale ne présente aucune lacune afin de pouvoir tester tous les scénarios. Pour les équipes de test, la tâche est particulièrement difficile lorsque les processus de test présentent des goulets d'étranglement qui entraînent des revers dans le développement.

Ainsi, de plus en plus d'entreprises adoptent les tests continus et doivent choisir les bons outils pour coordonner leurs équipes et harmoniser les processus. Par ailleurs, les différentes parties prenantes, les développeurs et les équipes de tests doivent pouvoir collaborer et communiquer pour accélérer la livraison et permettre la réalisation de tests à grande échelle.

Les tests continus sont un élément essentiel du cycle de vie du développement logiciel. Ils aident les entreprises à accélérer la mise sur le marché de leurs applications web et mobiles tout en leur permettant d'éliminer les défauts au plus tôt.

Bénéfices clés

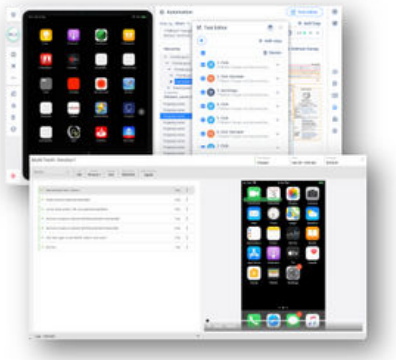


Accélérez la mise en production d'applications de qualité

- Mise à l'échelle des tests automatisés pour répondre à l'augmentation des demandes et réduire les délais de vérification.
- Tests en toute sécurité sur des appareils et des navigateurs réels multi-fournisseurs, quelque soit le système d'exploitation et sa version pour réduire la fragmentation.
- Tests mobiles, web, de performance et d'accessibilité sur une seule et même plateforme et dans le cadre de tests fonctionnels.

Simplifiez la création et débogage des tests

- Enregistrement des tests en un clic et export vers votre environnement de développement intégré (IDE) dans le langage de votre choix pour de meilleurs tests d'unité et de régression.
- Création de tests par des personnes qui connaissent le mieux les applications, sans aucune formation technique ni expérience de programmation.
- Utilisation des outils de débogage pour éliminer les défauts directement dans le module d'exécution de test et de validation des tests automatisés.



Testez à l'échelle de l'entreprise

- Réalisation des tests dans le Cloud pour partager des appareils et des navigateurs entre les régions et permettre à vos équipes d'y accéder en toute sécurité depuis n'importe où.
- Gestion des appareils et navigateurs à partir d'une interface centralisée sur laquelle les gestionnaires de Cloud mettent à jour les versions des applications et des systèmes d'exploitation.
- Utilisation d'un Cloud sur site protégé par vos pare-feux et vos paramètres de sécurité ou un Cloud SaaS avec des protections ISO 27001 et Soc-2 pour des tests en toute sécurité.

Fonctionnalités clés

Développement de tests

Créer des scripts de test robustes et stables avec des méthodes avancées d'identification telles que XPath et Object Spy, sans avoir de compétences en programmation.

Exécution à grande échelle

Exécuter des tests en parallèle sur plusieurs navigateurs et appareils mobiles à partir d'une seule et même plateforme.

Tests autonomes

Automatiser les tests d'intégrité et accélérer la création des tests plus rapidement, sans aucune compétence en programmation.

Analyses des données

Obtenir des informations de qualité de bout en bout pour apporter des améliorations avec la solution Digital.ai Test Analytics.

Tests de performance

Analyser les performances en simulant différents serveurs et en évaluant les transactions et l'indice de rapidité des livraisons.

Tests d'accessibilité

Tester le lecteur d'écran et les gestes pour proposer des sites web et des applications accessibles aux personnes handicapées.

digital.ai™ application security™

Digital.ai Application Security

Empêcher les acteurs malveillants de modifier les applications que vous créez en ajoutant des briques de protection à votre plateforme DevOps boostée par l'IA.

La solution Digital.ai Application Security relève les défis auxquels sont confrontés les propriétaires d'applications et les RSSI. Le principal avantage que nous offrons est la protection de cas pratiques de contournement du périmètre de sécurité que vos applications contiennent. Nous y parvenons en brouillant le code. Comment procédons-nous ? Nous prenons le code non protégé et l'intégrons, avec le plan de protection que vous créez (ou que nous créons pour vous), dans un moteur qui produit le code protégé. L'application protégée contient un code brouillé qui s'exécute comme prévu à l'origine, mais qui est pratiquement illisible par les acteurs malveillants, même après avoir été passé dans un désassembleur.

Ainsi, vous pouvez créer autant de personnalisations et ajouter autant de protections que vous le souhaitez à votre plan de protection, ou utiliser notre option de configuration automatique pour utiliser un plan de protection prédéfini (qui ne nécessite aucune personnalisation ou configuration) afin de brouiller automatiquement vos applications. L'option de configuration automatique vous permet de créer plus rapidement des applications protégées.
Le deuxième moyen que nous utilisons pour protéger les applications de nos clients consiste à ajouter des techniques anti-sabotage. Par anti-sabotage, nous entendons principalement la capacité à détecter deux conditions. Tout d'abord, nous pouvons détecter l'exécution de votre application dans un environnement non sécurisé qui pourrait permettre sa modification. Ces types d'environnements incluent par exemple les débogueurs, les émulateurs ou les appareils débridés. Ensuite, nous pouvons détecter la modification du code de votre application. Des protections anti-sabotage peuvent être ajoutées lors de sa construction sur site ou par Digital.ai dans le Cloud.

Par ailleurs, nous vous offrons également une visibilité sur 1) les attaques sur vos applications et 2) les tentatives d'exécution de vos applications dans des environnements non sécurisés. Par exemple, si un acteur malveillant tente de modifier votre code, vous recevrez une alerte. Vous verrez également de nombreux détails sur le lieu, l'appareil, le système d'exploitation et le navigateur dans lesquels la modification a eu lieu. L'adresse IP de l'appareil et l'emplacement géographique de l'acteur malveillant vous seront également communiqués, ainsi que l'heure à laquelle la modification a eu lieu et l'heure à laquelle elle a été détectée. Enfin, vous verrez le navigateur, l'agent utilisateur dans ce navigateur, l'URL où la modification a eu lieu et le nom du script spécifique qui a été modifié.

Associées à notre plateforme DevOps boostée par l'IA, ces protections sont ajoutées à vos applications sans ralentir leur processus de développement ou les applications elles-mêmes, tout en empêchant que vos applications soient utilisées comme vecteurs d'attaque pour voler votre IP, vos données
client ou vos revenus.

Bénéfices clés : protéger, surveiller, réagir

Protéger vos applications en intégrant la sécurité dans leur processus de développement

Protégez le code, les clés et les données de vos applications mobiles, Web et de bureau.

- Brouiller le code pour empêcher la rétro-ingénierie.
- Empêcher la modification en détectant les environnements non sécurisés et les modifications de code.
- Configurer des protections personnalisées ou automatisées sur site ou dans le Cloud.

Surveiller en bénéficiant d'une visibilité sur les applications à risque

Gagnez en visibilité sur les situations où les applications sont à risque.

- Générer des rapports autonomes ou intégré aux outils SOC (Security Operations Center) existants.
- Créer des journaux indexables.
- Identifier les mécanismes de protection activés.

Réagir en répondant automatiquement aux menaces

Intervenez automatiquement et en temps réel sur les menaces avec Runtime Application Self-Protection (RASP).

- Imposer l'authentification renforcée.
- Modifier les fonctions des applications.
- Forcer l'arrêt des applications qui sont attaquées.

Fonctionnalités clés

Réseau de protection

S'assurer que les pirates doivent démanteler chacune de vos protections simultanément pour attaquer votre application via l'application du réseau de protections.

Protection des clés et des données

La cryptographie en boîte blanche conforme à la norme FIPS 140-2 pour les clés privées garantit la sécurité de vos communications même si vos applications sont piratées.

Prise en charge de la solution Application Security dans plusieurs systèmes d'exploitation

Intégrer la sécurité aux applications codées pour la plupart des systèmes d'exploitation, notamment iOS, WatchOS, tvOS, Android, Mac, Windows et Linux.

Ajout de la solution Application Security à la plateforme DevOps boostée par l'IA

Digital.ai propose des tests de fonctionnement et de performance pour vos applications sécurisées, ainsi que des informations basées sur l'IA sur les tendances d'attaques.

Prise en charge de la solution Application Security sur plusieurs plateformes

Intégrer la sécurité aux applications mobiles, aux clients Web et aux applications de bureau.

Ajout de protections dans le Cloud ou sur site

Appliquer vos propres protections personnalisées sur site ou demander à ce qu'elles soient ajoutées pour vous automatiquement dans le Cloud.

Prise en charge de la solution Application Security dans plusieurs langages de développement

Intégrer la sécurité aux applications codées en C, C++, C#, Java, Javascript, HTML5 et Kotlin.

Détection des paquets malveillants

Se protéger contre les logiciels espions, les enregistreurs de frappe et les nombreux types de logiciels malveillants grâce à une protection dynamique.